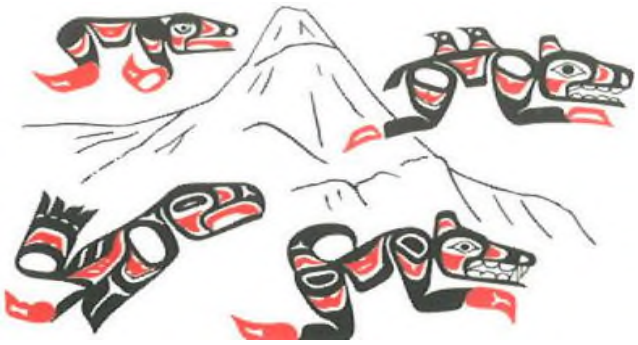
Gitsegukla Band
Information Management
Policy Manual



Version: March 2018

Signature Page

(All employees must comply with Gitsegukla Band Information Management Policies)

Instructions to Employee: All Gitsegukla Band managers and employees are required to read the Gitsegukla Band Information Management Policies listed in this document.

If you have trouble locating the policies, let your supervisor know.

Direct questions about Gitsegukla Band Information Management Policies to your supervisor.

Employee's Name: _____

Employee's Signature: _____ Date: _____

(My signature indicates I have read the information management policies and my questions have been answered. I understand I must comply with procedures and requirements of the policies. Failure to comply with the information management policies may result in disciplinary actions as outlined in the Human Resource Policy: Discipline, Termination and Resignation of Employees).

(The original Gitsegukla Band Information Management Policy Manual signature page is retained in the employee's Personnel File. Provide a copy to the employee.)

INTRODUCTION

The purpose of this Information Management Policy Manual is to provide guidance, assistance, and an accountability framework to the users of information created, maintained and retained by the Gitsegukla Band. Objectives are:

- To ensure the integrity of the information system, especially as it relates to financial information;
- To provide guidance on effective recordkeeping practices; and
- To provide guidance on the implementation of information privacy practices.

The users include Gitsegukla Band Council, the Financial Administrator, the Band Manager, Program Managers/Supervisors, and other employees.

The Information Management Policy Manual is reviewed after the annual audit to accommodate changes to the information system or implementation of new policies or procedures. The manual will be reviewed by the Finance and Audit Committee based on input from staff. Council will make approval of revisions to the Information Management Policy Manual.

A Finance and Audit Committee delegate is appointed by the Band Manager for processing all changes to the Information Management Policy Manual and distributing revisions to the Finance and Audit Committee Members, Band Manager, and Program Managers/Supervisors.

The Information Management Policy Manual will be available for review by all employees and members of Gitsegukla Band.

The Information Management Policy Manual is based on the sample statement of policy and procedures ("SPP") provided to First Nations that meet requirements contained in both the Financial Management Systems/Standards established by the First Nations Financial Management Board ("FMB") under the *First Nations Fiscal Management Act* ("FNFMA").

Using Policy Process Maps

Some of the policies that appear in this document are accompanied by process maps, which are visual representations of procedures and responsibilities. These are meant to assist the reader in understanding specific policies, but are not meant to provide a complete picture of all steps and details involved. The process maps should always be read along with the accompanying procedures in order to understand all of the details and required steps in a given policy.

CONTENTS

DEFINITIONS

“Classification” is the process of categorising records according to a predetermined hierarchy or scheme. Functional-based classification is the arrangement of records based on the business functions and activities of the Gitsegukla Band. This allows the Council to understand the records collected and created related to each business process / activity and how that record is used.

“Information” is knowledge communicated or received and may be any documentary material regardless of communications source, information format, production mode or recording medium.

“Information Security” refers to the physical, electronic and policy instruments that are used to protect information from unauthorized access (protecting confidentiality), unauthorized use (protecting integrity), unauthorized modification (also protecting integrity) and unauthorized destruction (protecting availability).

“Officers” means the Band Manager, Financial Administrator, Tax Administrator or any other employee of the Gitsegukla Band designated by the Council as an Officer;

“Personal information” refers to all information that reveals factual or subjective elements of knowledge about an identifiable individual. In addition to the basic elements that are commonly used to identify and interact with an individual - such as the individual’s name, gender, physical characteristics, address, contact information and identification and file numbers - it also includes criminal, medical, financial, family and educational history as well as evaluative information and other details of the individual’s life.

“Privacy Protection” refers to the decisions made by Gitsegukla Band in regards to the acceptable ways to collect, create, use, share/disclose, retain, protect and dispose of the Personal Information that it needs for its administrative and operational needs.

“Record” is a special form of information, and for the purposes of this policy refers to information created, received, and maintained by the Gitsegukla Band for business purposes or legal obligations, which enable and document decision-making, and support Gitsegukla Band reporting, performance and accountability requirements. A record may be electronic or hardcopy paper based.

“Recordkeeping” is a framework of accountability and stewardship in which records are created or acquired, captured, and managed as a vital business asset and knowledge resource to support effective decision-making and achievement of results for the Gitsegukla Band.

“Repository” refers to a preservation environment for a record. It includes specified physical or electronic storage space and the associated infrastructure required for its maintenance. Business rules for the management of records in a Repository need to be established, and there must be sufficient control for the resources to be authentic, reliable, accessible and usable on a continuing basis.

“Rollback Procedure” means the ability to restore system to previous configuration prior to change, with documented procedures and steps to complete the process.

“Virtual Private Network” means a Virtual Private Network (“VPN”) which is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

1. INFORMATION TECHNOLOGY

Manual: Information Management		No:	IM01.02
Section:	General	Issued:	March 31, 2018
Issue to:	All Manual Holders	Page:	1 of 3
		Replaces:	
Issued by:	Chief and Council	Issued:	

Policy

The Gitsegukla Band's information systems will support its operational requirements and have appropriate safeguards and monitoring processes in place to adequately protect the Gitsegukla Band's information.

Purpose

The purpose of this policy is to ensure that information system integrity, specifically as it relates to the financial administration system, is maintained and supports the strategic and operational requirements of the Gitsegukla Band.

Scope

This policy applies to all staff involved in the selection, implementation, operations, or ongoing maintenance of the Gitsegukla Band's information systems. This includes the Band Manager, and information technology staff.

Responsibilities

Council is responsible for:

- Establishing and implementing documented procedures for information technology used by the Gitsegukla Band in its operations.

The **Band Manager** is responsible for:

- Ensuring that controls are in place over information technology, whether performed by an internal staff member or outsourced to an external organization;
- Monitoring the performance of internal and/or external information technology professionals.

The **Information Technology Professional** is responsible for:

- Maintaining the integrity of information systems within the Gitsegukla Band.

Procedures

Planning and evaluation

- The Council, with the assistance of the Band Manager and input from information technology staff/partners, will ensure that information systems are developed that support the Gitsegukla Band's strategic plan and operations.

- When there are no individuals internally with the requisite technical skills to identify information technology requirements or evaluate options, the Band Manager will seek advice from a qualified external individual or organization.

Outsourcing

1. Subject to the Procurement Policy, the Band Manager is responsible for the selection of contractors providing information technology services, the definition of services in their contracts, establishing service level agreements and the administration of the contracts.
2. Specific items which should be included in the procurement of information technology services and final contract with the chosen provider include:
    a. A requirement that the service provider submits regular reports of all work performed on the Gitsegukla Band's information systems;
    b. A requirement that outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information;
    c. Access by outsourced parties to Gitsegukla Band information is provided on a 'need to know basis' only.

Data management

1. Subject to the Records and Information Policy, data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.
2. All sensitive, valuable, or critical information/data residing on the Gitsegukla Band's information technology systems must be periodically backed-up. Backups will occur incrementally on a daily basis, with full backups on a weekly and monthly basis.
3. Backup drives must be stored in a secure location with access limited to the Band Manager and limited other staff as appropriate. Ideally, backup drives will be securely stored at an offsite location that is easily accessible to individuals with authorized access.
4. Backup drives will be retained for a period of 24 months before being overwritten or deleted.

Access management

1. All individuals requiring access to Gitsegukla Band information systems will have unique user identification. Shared user IDs or passwords will not be permitted.
2. Requests for access to the Gitsegukla Band's network, accounting system, or other access restricted information system must include a description of an employee's role and rationale for the level of access required. Signed or e-mail approval must be obtained from the Band Manager (or designate).
3. User ID and password are required for access to the network and other critical programs/areas such as the accounting system. Automatic authentication using scripts or macros inserting user IDs and/or passwords are prohibited.
4. Individuals will be given access privileges to the extent necessary to fulfill their individual job function and no more. Systems and applications should not be configured with unrestricted access to all data.
5. When an individual or contractor is terminated or ends employment with the Gitsegukla Band, their user IDs must be disabled immediately.
6. Support personnel must notify the user when attempting to take control of a workstation. All instances where specific software is loaded to remotely control a workstation must be removed when the support function is completed. The use of the remote control software must be in accordance to applicable agreements.

Information system security

1. Security tools and techniques are implemented to enable restrictions on access to programs and data.

2. Security tools and techniques are administered to restrict access to programs and data.
3. Each computer resource must have an approved antivirus program installed.
4. The antivirus program must not be disabled and must be configured to scan all programs and files upon execution and must have real time protection enabled. If encrypted and password protected files cannot be virus checked, it is the responsibility of the user to ensure that virus checking takes place whenever this protection is removed;
5. Antivirus files must be updated on the network every two weeks or whenever a new threat is identified.
6. Network firewalls must be configured to support a 'least-privilege' approach to security, allowing only specific systems, services and protocols to communicate through the network perimeter. Logical and physical access to these systems must be limited strictly to those personnel with specific training and authorization to manage the device. Additionally, the following Firewall standards must be addressed:
    a. Firewall and proxy servers must be securely installed;
    b. Detailed firewall logs must be maintained;
    c. Alerts must be raised if important services or processes crash.

Change management

1. All new data structure and modifications to data structure will be tested before implementation.
2. All computers, hardware, software and communication systems used for a production environment must employ a documented change control process. The change management process should include the following activities:
    a. The data structure is consistent with the needs of the Gitsegukla Band;
    b. Description and rationale for the new network, hardware, communication and systems software change and how it is consistent the needs of the Gitsegukla Band;
    c. An assessment of any risks involved with the change;
    d. Roll-back considerations;
    e. Implementation considerations;
    f. A description of the testing required;
    g. Approval from the Band Manager;
    h. Communication of changes to Gitsegukla Band staff as appropriate.

Monitoring

1. Only approved and authorized programs will be implemented onto Gitsegukla Band information management systems. Periodic reviews of the workstations and the system will take place to monitor compliance with this requirement.
2. A log of staff, their user IDs, and their access levels within Gitsegukla Band information systems will be maintained. On an annual basis, the Band Manager will review the log to ensure users and the associated access rights are appropriate. Access rights that will be monitored include the following:
    a. User access management (i.e. the accounting system);
    b. Third party access (i.e. outsourced information technology professionals);
    c. Network access and file sharing;
    d. Remote and VPN access.
3. Network system performance is monitored on a regular basis.
4. The firewalls must be monitored daily and their functionality audited semi-annually.

References and Related Authorities

1. FMB's Financial Management System Standards

a. Standard 19.8 - Information Technology Controls

2. FMB's Financial Administration Law Standards
    a. Standard 17.6.2 - Information Technology Controls

Attachments

None

2. RECORD AND INFORMATION MANAGEMENT

Manual: Information Management Policy		No:	IM01.03
Section:	General	Issued:	March 31, 2018
Issue to:	All Manual Holders	Page:	1 of 4
		Replaces:	
Issued by:	Chief and Council	Issued:	

Policy

Records are a special form of information that is created, received, and maintained by the Gitsegukla Band for business purposes or legal obligations, which enable and document decision-making, and support Gitsegukla Band reporting, performance and accountability requirements. Records must be created and collected, organized, retained, and safeguarded in a manner that enables their long-term availability, understandability and usability.

Purpose

The purpose of the policy is to provide guidance on effective Recordkeeping practices that enable the Gitsegukla Band to create and acquire; manage; and, protect the integrity of its records that support its decision-making, and support Gitsegukla Band reporting, performance and accountability requirements.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of the Gitsegukla Band and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all records created and acquired by the Gitsegukla Band regardless of format (i.e., both electronic and hardcopy paper records).

Responsibilities

Council is responsible for:

- Establishing and implementing documented procedures for records management within the Gitsegukla Band.

The Band Manager is responsible for:

- Implementing appropriate Recordkeeping practices,
- Ensure appropriate safeguards of the Gitsegukla Band's records;
- Ensuring compliance with the established records retention and disposition schedule and overseeing the disposition process;
- Ensuring that employees and any contractors or volunteers performing services on behalf of the Council are fully knowledgeable of their responsibilities as they relate to Recordkeeping practices.

Employees, contractors and volunteers are responsible for:

- Complying with the established records management policy.

- Immediately reporting to their supervisor any potential breach related to compliance with the record keeping policy, including the incidents in which the safeguarding of records may have been compromised.

Procedures

Accountability

1. Each record shall have a designated steward that ensures the Recordkeeping framework outlined in this policy is applied to the record. All employees, contractors, or volunteer that are in custody of a record must ensure it is managed in accordance with this policy.
2. Permanent records such as operations manuals, policies, and procedures will be reviewed and updated by the steward periodically, but at least every two years, or more frequently as required.
3. Records under the stewardship of an employee or any contractor or volunteers that is departing must be formally transferred to another employee through a knowledge transfer process. This process should include information on the types of records to be transferred, how the records are organized, in which Repository the records are kept, and required safeguards.

Creation and Collection

1. All important activities and decision-making processes of the Gitsegukla Band should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect the Gitsegukla Band from liability.
2. All information at its time of creation or collection should be assessed to determine if it supports Council's business purposes or legal obligations, and enables decision-making. If determined to be a record its management should comply with the procedures outlined within this policy.
3. The Gitsegukla Band's records shall be created using the most appropriate application to ensure that they adequately support the objectives for which they are created and can easily be used by those who need them to perform their duties – i.e., using MS Excel instead of MS Word to develop spreadsheets with financial figures, etc.
4. The Gitsegukla Band's records shall contain all the information necessary to achieve the objectives for which each of them is created; yet their contents shall be limited to only what is necessary to achieve those objectives. This should include limiting the information collected through forms to only that which is required.
5. Whenever possible, the record shall contain information about one single function or activity to facilitate information Classification, organization, retention and retrieval.
6. The Gitsegukla Band's records shall be legible, written in plain language and adapted to their specific audience.
7. Only one copy of each record should be created or collected. When creating or collecting a record, individuals should first check to see if the record is already in existence. In instances of multiple copies of the same record, copies should be securely disposed in accordance with the requirements of this policy.

Organization and Classification

1. A Classification plan structure shall be implemented based on the Gitsegukla Bands functions and activities, with records stored in accordance with the activity and/or function that it supports. This Classification plan should be used to support the filing system for both electronic records and hardcopy paper-based records.
2. Records should be subject to a consistent naming convention, with the name of the record including the title, version (v. XX) and date (DD/MM/YYYY).
3. The title of the document should be short but meaningful.

4. The title may contain multiple words, and should be ordered from most specific to less specific related to the business activity or function.
5. Common words such as ‘draft’ or ‘letter’ should not be at the start of the title.
6. An official Repository shall be identified and designated for each record, in which the record must be stored. The number of record repositories should be limited and be consistent to support the format and type of record.
7. Records should be made accessible, shared and re-used to the greatest extent possible, subject to technological, legal policy and security restrictions.

Maintenance, Protection and Preservation

1. Records must be protected and stored in the appropriate repositories in a way that preserves their long-term availability, understandability and usability.
2. Backups should be taken of all electronic records on a regular basis and stored in a physical location separate from the location of the original records.
3. Any records that are only in hardcopy paper-based format should be assessed to determine if they need to be scanned or if other physical security measures need to be taken (e.g. use of fire/water proof cabinets) to ensure their long-term availability.
4. Records that contain Personal Information or information of a confidential nature related to the Council, or a third party, such as the confidential financial information related to a business, should be labelled as CONFIDENTIAL.
5. Confidential records should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:
    a. For electronic records, confidential records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Confidential records should not be emailed ‘in the clear’ without appropriate protection.
    b. For hardcopy paper-based records, confidential records should be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be offsite.

Retention and Disposition

1. The Gitsegukla Band records shall be retained for the period specified in the records and information retention and disposition schedule, as outlined in Appendix A. They shall be disposed of in a manner that prevents their reconstruction (for paper based records) or recovery (for electronic records).

References and Related Authorities

1. FMB’s Financial Management System Standards
    a. Standard 19.8 - Information Technology Controls
2. FMB’s Financial Administration Law Standards
    a. Standard 17.6.2 - Information Technology Controls

Attachments

Appendix A – Document Retention Periods

3. INFORMATION PRIVACY

Manual: Information Management Policy		No:	IM01.04
Section:	General	Issued:	March 31, 2018
Issue to:	All Manual Holders	Page:	1 of 5
		Replaces:	
Issued by:	Chief and Council	Issued:	

Policy

Ensuring the privacy of Personal Information provided to the Gitsegukla Band by individuals is essential to not only ensure compliance with legislative requirements such as those outlined in the Personal Information Protection and Electronic Documents Act or substantially similar provincial legislation, but also to ensure continued stakeholder confidence in the Gitsegukla Band and that accountability is maintained.

Purpose

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within the Gitsegukla Band related to the collection, use, disclosure, retention, and safeguarding of Personal Information.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of the Gitsegukla Band and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all Personal Information created and acquired by the Gitsegukla Band regardless of format (i.e., both electronic and hardcopy paper records).

Responsibilities

Council is responsible for:

- Establishing and implementing documented procedures for privacy and the management of Personal Information within the Gitsegukla Band.

The **Band Manager** is responsible for:

- Ensuring compliance with the established information privacy policy.
- Developing and maintaining standards, policies and procedures that support the objectives of the Gitsegukla Band's privacy program;
- Ensuring that all the activities of the Gitsegukla Band are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the Privacy Officer will:
    - Provide training and awareness on Privacy Protection.
    - Ensure that community members are aware of their rights as they relate to privacy, including their right of access to, and the right to request the correction of, all the Personal Information which is kept about them by the Gitsegukla Band.
    - Act as an expert resource on privacy matters within the Gitsegukla Band.

    - Conduct periodic reviews of the Gitsegukla Band's activities that involve the collection, use, disclosure, retention, and safeguarding of Personal Information.
- Investigating all complaints regarding the collection/creation, accuracy, use, sharing/disclosure, protection, retention and destruction of Personal Information and reporting the results to the appropriate managers and, where warranted, to Council;
- Recommending changes to policies, procedures and practices in response to the issues raised in the complaints; and
- Responding in writing to the requests for access to, and correction of Personal Information submitted by employees and community members within thirty calendar days from the date of the receipt.

Employees, contractors and volunteers are responsible for:

- Complying with the established information privacy policy; and
- Immediately reporting to their supervisor privacy breaches of which they become aware.

Procedures

Accountability

1. The Gitsegukla Band is responsible for Personal Information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Identifying Purpose

1. The purposes for the collection of Personal Information should be communicated to individuals at or before the time of collection. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.
2. Personal information should be collected directly from the individual whenever possible.
3. Persons collecting personal information must be able to explain to individuals the purposes for which the information is being collected.

Consent

1. With limited exceptions, the Gitsegukla Band must obtain consent from an individual before collecting their personal information. Consent requires that the individual is advised of the purposes for which the information is being collected and how it will be subsequently used and disclosed.
2. Consent must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Consent must not be obtained through deception.
3. Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances. For example, legal or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Consent may be sought from an individual's authorized representative in certain cases, for example, when an individual is seriously ill, mentally incapacitated, a minor, or has died.
4. If personal information is intended to be used or disclosed for a new purpose not identified during the original collection, and not related to the original purpose of the collection, the consent of the individual must be obtained.
5. Individuals can give consent in many ways. For example:

a. a form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

b. consent may be given orally; or,

c. consent may be given through electronic means.

6. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Gitsegukla Band must stop using the individual's personal information within a reasonable time period and inform the individual of this time period and the implications of such withdrawal.

Limiting Collection

1. The Gitsegukla Band cannot collect personal information indiscriminately. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified.

Limiting Use, Disclosure and Retention

1. The Gitsegukla Band may only use or disclose personal information for the purpose for which it was collected, unless:
    a. The use or disclosure of the personal information is consistent with the original collection of the personal information;

    b. The consent of the individual is obtained; or,

    c. It is for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information.

2. Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.
3. Identifiable personal information must only be used and disclosed if required. For instance, consider if reports, research, or audits/assessments can be done through de-identified or anonymous data.
4. Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous in accordance with the Gitsegukla Band's retention and disposition schedule.

Accuracy

1. The Gitsegukla Band shall take all reasonable steps to ensure that personal information that is used to make a decision on an individual is as accurate, up-to-date and complete as possible to minimize the possibility that inappropriate information may be used to make a decision about the individual.

Safeguards

1. Personal information should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:
    a. For electronic records containing personal information, the records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Personal information should not be emailed 'in the clear' without appropriate protection.

b. For hardcopy paper-based records, containing personal information, the records should be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be taken offsite.

2. The Gitsegukla Band must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.
3. Care must be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Openness

1. The Gitsegukla Band must be open about its policies and practices with respect to the management of personal information. Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information must be made available in a form that is generally understandable.
2. The information made available should include:
    a. the name or title, and the address, of the Band Manager, who is accountable for the Gitsegukla Band's policies and practices, and to whom complaints or inquiries can be forwarded;
    b. the means of gaining access to personal information held by the Gitsegukla Band; and,
    c. a description of the type of personal information held by Gitsegukla Band, including a general account of its use.

Individual Access

1. When requested, an individual must be informed if the Gitsegukla Band holds personal information about the individual and provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
2. The identity of an individual must be authenticated before discussing their personal information with them.
3. When requested, the Gitsegukla Band must provide an individual with access to their personal information within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable.
4. Individuals who are given access to their personal information may:
    a. request correction of the personal information where the individual believes there is an error or omission therein;
    b. require that a notation be attached to the information reflecting any correction requested but not made; and,
    c. require that any person or body to whom that information has been disclosed for use for a decision-making process within two years prior to the time a correction is requested or a notation be notified of the correction or notation.
5. In certain situations, the Gitsegukla Band may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that:
    a. is prohibitively costly to provide;
    b. contains references to other individuals;
    c. cannot be disclosed for legal, security, or commercial proprietary reasons; or,

d. is subject to solicitor-client or litigation privilege.

Challenging Compliance

1. The Gitsegukla Band must ensure that a process exists to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.
2. The Gitsegukla Band must investigate all complaints. If a complaint is found to be justified, the Gitsegukla Band will take appropriate measures referred to in the Gitsegukla Governance Policy Section 4.2, including, if necessary, amending its policies and practices.

References and Related Authorities

1. FMB's Financial Management System Standards
    a. Standard 12.6 - Human Resource records
    b. Standard 19.0 - Risk Management
    c. Standard 23.0 - Records and Information
2. FMB's Financial Administration Law Standards
    a. Standard 21.0 - Records and Information

Attachments

None

Appendix A – Document Retention Periods

Record or information	Duration
General Gitsegukla Band governance records	
All Gitsegukla Band bylaws, amendments to the bylaws, the Gitsegukla Band constitution, and membership resolutions	Permanent
Appointments and terms of appointments	Permanent
Applicable legislation, agreements, funding arrangements, council commitments, land codes in force, financial administration codes for oil & gas monies management	Permanent
The Gitsegukla Band's Financial Administration Law	Permanent
The Gitsegukla Band's Property Taxation Law or By-law	Permanent
The Gitsegukla Band's Borrowing Law	Permanent
Minutes from the meetings of the Council and all council committees, annual reports, debenture records and council, committee and membership records, public notices, records of incorporation, corporate seal	Permanent
Legal files and papers	
Customer and supplier contracts and correspondence related to the terms of the contracts	7 years beyond life of contract
Contractual or other agreements (e.g., contribution, impact benefit, trust) between the Gitsegukla Band and others and correspondence related to the terms of the contracts	7 years beyond life of the contract
Papers relating to major litigation including those documents relating to internal financial misconduct	5 years after expiration of the legal appeal period or as specified by legal counsel
Papers relating to minor litigation including those documents relating to internal financial misconduct	2 years after the expiration of the legal appeal period
Insurance policies including product or service liability, council and Officers liability, general liability, and third-party liability, property and crime coverage	7 years after the policy has been superseded
Documents pertaining to the purchase, sale or lease of property	Permanent
Documents pertaining to equity investments or joint ventures	Permanent
Human Resources	
Personnel manuals and procedures	Permanent
Organization charts	Permanent
Where there is a pension plan (excluding RRSP plans): Original plan documents; records of pensionable employee service and eligibility; associated personal information including name, address, social insurance number, pay history, pension rate	7 years after the death of the employee or employee's spouse in the case of spousal eligibility
Letters of offer and individual contracts of employment	2 years after termination of the employee
Signed Code of Conduct obligations and signed Conflict of Interest declarations	2 years after termination of the employee

Record or information	Duration
Attendance records	2 years after termination of the employee
Financial information such as payroll history including RRSP contributions, commission and bonus history	2 years after termination of the employee
Medical information	2 years after termination of the employee
Job descriptions	2 years beyond the period to which it applies
Performance assessments	2 years beyond the period to which it applies
Applications, resumes, and correspondence related to individuals not hired	2 years beyond the period to which it applies
Financial records	
Operations manuals, procedures, and internal control guidelines	Permanent
Signed annual financial statements and corresponding signed independent auditor reports	Permanent
Internal reports, including but not limited to: Reviews Annual operations report Special purpose reports Internal audit reports	10 years
Accounting documentation, including but not limited to: General ledgers, general journals, financial records and supporting documentation Monthly and quarterly financial statements Monthly and quarterly management reports Month / Quarter / Year-end Financial Closing and Reporting work papers Financial institution account statements and reconciliations Cancelled cheques and cash register tapes Invoices Annual budgets Multi-year financial plans	8 years
Asset management documentation, including but not limited to: Tangible capital asset register Reserve fund reports Life cycle planning Capital project budgeting Contract and tendering provisions	8 years beyond completion of the project or asset utilization
If applicable, property taxation related documentation, including but not limited to: Property tax working papers Tax roll Tax filings	8 years

Record or information	Duration
Operational records	
Operations manuals, policies and procedures	Permanent
Original patents, trademarks, and copyrights	7 years after the expiration of the right
Customs documents	7 years
Annual physical inventories	Permanent
Safety committee minutes, inspection reports and related action reports	10 years